# PCI PA-DSS Implementation Guide

For Verifone **VX 820** and
Verifone **VX 825**
terminals using the
Verifone iPOS payment core **I02.01** Software

## Revision History

| Version | Name | Date | Comments |
|---|---|---|---|
| 1.00 | M. Oscarsson | 2012-01-26 | Initial version |
| 1.01 | M. Oscarsson | 2012-02-16 | References updated with “Point Transaction Systems AB Point iPOS Users Guide”<br>Chapter 2.5, Requirement 10, section c updated to state that iPOS message SR_MESSAGE is used to transmit the Audit Trail<br>Chapter 1, Note 1 updated to stat that the Implementation Guide should be distributed to all relevant payment application users. |
| 1.02 | M. Oscarsson | 2013-02-08 | Annual review, no change |
| 2.00 | M. Oscarsson | 2013-10-03 | Graphical layout changed |
| 3.0 | Jan Sternelind | 2015-11-06 | Changed core version into I02.01<br>Change reference into PA-DSS 3.1<br>Graphical layout changed into Verifone |
| 3.01 | Jan Sternelind | 2015-11-13 | Corrected location of log and S&F files |
| 3.02 | Björn Löfroth | 2015-12-10 | Corrected description of where to find this document. |
| 3.03 | Jan Sternelind | 2016-01-14 | Updated with old Revision history<br>Added Appendix A, Version methodology |
| 3.04 | Jan Sternelind | 2016-01-14 | Removed reference to VX iPOS – Version methodology<br>Changed reference from VX iPOS – Version methodology into see Appendix A.<br>Renumbered reference list |
| 3.05 | Jan Sternelind | 2016-01-21 | Updated 3.3 with that SNMP and passwords should change |
| 3.06 | Björn Löfroth | 2016-04-04 | Added link to corporate site for latest version of this document. |

## References

| Nbr. | Title | Version |
|---|---|---|
| 1 | Payment Card Industry – Payment Application Data Security Standard | 3.1 |
| 2 | Payment Card Industry – Data Security Standard | 3.1 |
| 3 | Point Transaction Systems AB - Point iPOS Users Guide | |
| 4 | Babs & CEKAB Security Requirements for an EFTPOS Terminal Version | 3.0 |
| 5 | Handling of card data in conformance with PCI DSS | 2.0 |
| 6 | iPOS Messages and Commands | 3.2 |
| 7 | Terminal Audit Logs File Format | 1.0 |
| 8 | Point Transaction Systems AB – Point iPOS Audit logging | 1.0 |
| 9 | NIST Special Publication 800-57 Part 1 | Revision 3 |

# Table of contents

# 1. Introduction

The Payment Card Industry Data Security Standard (PCI-DSS) defines a set of requirements for the configuration, operation, and security of payment card transactions in your business. If you use Verifone iPOS in your business to store, process, or transmit payment card information, this standard and this guide apply to you.

The requirements are designed for use by assessors conducting onsite reviews and for merchants who must validate compliance with the PCI DSS.

For more details about PCI DSS, please see the following link:
http://www.pcisecuritystandards.org

This guide is updated whenever there are changes in Verifone iPOS software that affect PCI DSS and is also reviewed annually and updated as needed to reflect changes in the Verifone iPOS as well as the PCI standards.
Please contact Verifone sales representative or customer support to retrieve the latest version of the document. Latest version of this document can also be found at www.verifone.se/sv/Sweden/OmVerifone/

The Payment Card Industry has also set the requirements for software applications that store, process or transmit cardholder data. These requirements are defined by the Payment Card Industry Payment Application Data Security Standard (PCI PA-DSS). In order to facilitate for you to get a PCI DSS assessment the Verifone iPOS software application has been approved by PCI to comply with the PCI PA-DSS requirements.

**Note:** This guide refers to Verifone iPOS terminals using the Verifone iPos Payment Core. The version of the Verifone iPos Payment Core is listed on the PCI web site “List of Validated Payment Applications” that have been validated in accordance with PCI PA-DSS. If you cannot find the version of the Verifone iPos Payment Core running on your Verifone iPOS on that list please contact our helpdesk in order to upgrade your terminal.
**http://www.pcisecuritystandards.org/**

This guide refers to Verifone iPOS Payment Core I02.01 used on the following PCI PTS approved hardware:

- Verifone VX820 PCI PTS approval number 4-40054
- Verifone VX825 PCI PTS approval number 4-10107

More information regarding the approved hardware can be found on the PCI web site “Approved PTS Devices” at
**http://www.pcisecuritystandards.org/**

**Document Use**

This PA-DSS Implementation Guide contains information for proper use of the Verifone iPOS application. Verifone Sweden AB does not possess the authority to state that a merchant may be deemed “PCI Compliant” if information contained within this document is followed. Each merchant is responsible for creating a PCI-compliant environment. The purpose of this guide is to provide the information needed during installation and operation of the Verifone iPOS application in a manner that will support a merchant’s PCI DSS compliance efforts.

**Note 1: Both the System Installer and the controlling merchant must read this document.**

**Note 2: This document must also be used when training ECR/vending machine integrators/resellers at initial workshops.**

# 2. Summary of PCI DSS requirements

This summary provides a basic overview of the PCI DSS requirements and how they apply to your business and the Verifone iPOS terminal.

## 2.1. Build and Maintain a Secure Network

**Requirement 1: Install and maintain a firewall configuration to protect cardholder data**

### *a. What the requirement says*

"Firewalls are devices that control computer traffic allowed between an entity's networks (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within an entity's internal trusted networks. The cardholder data environment is an example of a more sensitive area within an entity's trusted network.

A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employee Internet access through desktop browsers, employee e-mail access, dedicated connections such as business-to-business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

Other system components may provide firewall functionality, as long as they meet the minimum requirements for firewalls as defined in Requirement 1. Where other system components are used within the cardholder data environment to provide firewall functionality, these devices must be included within the scope and assessment of Requirement 1.", reference 2.

### *b. How your Verifone iPOS helps you meet this requirement*

Verifone iPOS is designed to operate in a network behind a firewall.

Verifone iPOS only requires the use of one port for communication between the terminal and ECR/vending machine.

### *c. What this means to you*

A common installation use RS232 communication and there is no Ethernet connection to the terminal available.

If you are using wireless technology you must install and maintain a firewall to protect your Verifone iPOS from someone hacking the wireless environment. Also, if your network connection allows inbound traffic you should use a firewall. The terminal should not be placed in an Internet accessible network zone ("DMZ").

In case a firewall is connected between the terminal and the ECR/vending machine the configurable TCP port must be opened to enable communication between the two. Only one port is necessary for communication between the terminal and ECR/vending machine. No other ports, services, components or other dependent hard- and software are required provided by the vendor or third parties

If the terminal is configured for Ethernet then the default port number is 8899 but it can be changed via the IposConf utility. Please refer to the user's manual.

The only required protocol for communication with the ECR/vending machine is the iPOS protocol.

For more information about setting up your firewall to work with Verifone iPOS, please refer to the manual supplied by your firewall vendor.

**Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters**

***a. What the requirement says***

"Malicious individuals (external and internal to an entity) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.", reference 2.

***b. How your Verifone iPOS helps you meet this requirement***

Verifone iPOS does not allow users to access any card holder data or sensitive authentication data. IP addresses for processors, terminal management systems and software download servers are protected by unique passwords per terminal and these passwords are changed on a daily basis. For more information about the level of passwords protection for Verifone iPOS maintenance menus please refer to "*Point Transaction Systems AB – Point iPos User's Guide", reference 3*

***c. What this means to you***

Since the password protection for the Verifone iPOS is handled entirely within the unit there is no need for you to take any action.

## 2.2. Protect Cardholder Data

**Requirement 3: Protect stored cardholder data**

***a. What the requirement says***

"Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should also be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending unprotected PANs using end-user messaging technologies, such as e-mail and instant messaging.

Please refer to the *PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms* for definitions of "strong cryptography" and other PCI DSS terms.", reference 2.

***b. How your Verifone iPOS helps you meet this requirement***

Verifone iPOS never stores full magnetic stripe data from the card. For offline transactions PAN and expiry date are stored encrypted using a unique key per transaction see section 3.2.

At transaction time PAN is truncated before it is stored, only the first 6 and last 4 digits are stored. For printout of receipts and reports the truncated PAN is sent to the ECR/vending machine.

All key handling is done by the acquirer and in the secure part in the application. The key management process and procedures are according to "*Babs & CEKAB Security Requirements for an EFTPOS Terminal Version 3.0*", reference 4, and "*Handling of card data in conformance with PCI DSS Version 2*", reference 5.

All the keys used for encryption of cardholder data and data-encryption in the application are under the Acquires control and always transferred and loaded encrypted and stored inside the safe parts of the terminal. The keys are double length DES keys and the encryption is triple DES and unique for each transaction.

#### *c. What this means to you*

For cards read by the Verifone iPOS magnetic stripe reader or chip card reader you do not have to take any action.

For voice referrals it is never allowed to write down or otherwise store PAN, expiration date or CVV2.

Since no keys or components in plain text are handled outside the secure part of the application no action is required regarding key management.

All handled card data or stored card data within the Verifone iPOS terminal is automatically deleted when the transaction is completed and no manual action is required by you for deleting cardholder data.

**Requirement 4: Encrypt transmission of cardholder data across open, public networks**

#### *a. What the requirement says*

"Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols continue to be targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments.", reference 2.

#### *b. How your Verifone iPOS helps you meet this requirement*

The Verifone iPOS encrypts card holder data using triple DES with a unique key per transaction.

#### *c. What this means to you*

If you are using a wireless network, WLAN, you must set up your wireless network to use WPA/WPA2 encryption for new installations. **N.B. WEP must not be used after June 30 2010.** The WLAN encryption is applied on top of the triple DES encryption, in order to be compatible the communication client must use strong cryptography, see reference 10 "NIST SP 800-57 Part 1".

If you connect to an external network without using WLAN you do not need to take any action.

Communication to host systems must be protected using strong encryption, for example VPN with 3DES using 168-bit keys or AES 256 or TLS version 1.2. This protection must be provided by the SACI provider as the terminal has no Ethernet connection in a standard installation.

## 2.3. Maintain a Vulnerability Management Program

**Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs**

#### *a. What the requirement says*

"Malicious software, commonly referred to as "malware"—including viruses, worms, and Trojans—enters the network during many business-approved activities including employee e-mail and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats. Additional anti-malware solutions may be considered as a supplement to the anti-virus software; however, such additional solutions do not replace the need for anti-virus software to be in place.", reference 2.

#### *b. How your Verifone iPOS helps you meet this requirement*

The Verifone iPOS cannot be used for e-mails or internet activities. All software downloaded to the terminal is controlled by Verifone, protected by a digital signature (MAC). These security measures prevent malicious software being installed onto your Verifone iPOS terminal.

#### *c. What this means to you*

You should install and maintain antivirus software which helps to protect your system. Make sure that this software is up to date as security threats change.

For the Verifone iPOS you do not need to take any action regarding antivirus software.

**Requirement 6: Develop and maintain secure systems and applications**

#### *a. What the requirement says*

"Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches, which must be installed by the entities that manage the systems. All systems must have all appropriate software patches to protect against the exploitation and compromise of cardholder data by malicious individuals and malicious software.

**Note**: *Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques.*", reference 2.

#### *b. How your Verifone iPOS helps you meet this requirement*

Verifone Sweden constantly works with the latest security findings and requirements throughout the life cycle of your Verifone iPOS. This includes automatic SW updates whenever necessary.

The Verifone iPOS software follow the versioning methodology described in document "VX iPOS – Version methodology", see Appendix A.

#### *c. What this means to you*

You should keep your system up to date with software updates, operating system updates, and any other security patches.

For the Verifone iPOS you do not need to take any action.

## 2.4. Implement Strong Access Control Measures

**Requirement 7: Restrict access to cardholder data by business need to know**

#### *a. What the requirement says*

"To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities.
"Need to know" is when access rights are granted to only the least amount of data and privileges needed to perform a job.", reference 2.

### *b. How your Verifone iPOS helps you meet this requirement*

The Verifone iPOS does not disclose any cardholder data. Sensitive authentication data is always encrypted when sent for authorization and never stored. PAN is always truncated when stored, thus only truncated PANs are sent to the ECR/vending machine for printouts of reports, logs or receipts.

### *c. What this means to you*

In case you have to do voice referrals you must never keep written copies or otherwise store copies of cardholder data. Also, you must never e-mail, fax etc card holder data.

For cards read by the Verifone iPOS magnetic stripe reader or chip card reader you do not need to take any additional security measures.

**Requirement 8: Identify and authenticate access to system components**

### *a. What the requirement says*

"Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for their actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users and processes.

The effectiveness of a password is largely determined by the design and implementation of the authentication system—particularly, how frequently password attempts can be made by an attacker, and the security methods to protect user passwords at the point of entry, during transmission, and while in storage.", reference 2.

### *b. How your Verifone iPOS helps you meet this requirement*

The Verifone iPOS does not allow access to critical data. The administrative access to the physical unit is protected by pre-expiree passwords that have to be changed at first login. The pre-expiree passwords must be changed when the system is activated the first time.

Requirement 8.3: The Verifone iPOS does not allow direct remote access to the system. But for remote updates via Terminal Management Systems the authentication used as part of an authenticated remote software distribution framework for the PED, should be evaluated by a QSA as part of any PCI DSS assessment.

### *c. What this means to you*

Since the Verifone iPOS does not allow access to critical data you do not need to take any action.

Requirement 8.3: Ask your QSA to include the remote update process in the PCI DSS assessment.
All remote access originating from outside your network to the payment application must use two-factor authentication in order to meet PCI DSS requirements

**Requirement 9: Restrict physical access to cardholder data**

***a. What the requirement says***

"Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted. For the purposes of Requirement 9, "onsite personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are physically present on the entity's premises. A "visitor" refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day. "Media" refers to all paper and electronic media containing cardholder data.", reference 2.

***b. How your Verifone iPOS helps you meet this requirement***

The Verifone iPOS physically prevents by encryption and truncation users to access cardholder data.

***c. What this means to you***

For your Verifone iPOS you do not need to take any action.

## 2.5. Regularly Monitor and Test Networks

**Requirement 10: Track and monitor all access to network resources and cardholder data**

***a. What the requirement says***

"Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.", reference 2.

***b. How your Verifone iPOS helps you meet this requirement***

The Verifone iPOS keeps a log for the 1000 latest transactions. This log contains truncated PANs. No cardholder data is accessible from the Verifone iPOS.

The Verifone iPOS also keeps an Audit Trail to track changes to system level objects.

The Verifone iPOS central logging mechanism relies on logging of transmitted iPOS messages called SR_MESSAGES .

***c. What this means to you***

For the transaction log you do not need to take any action since no cardholder data is accessible.

For the Audit Trail there are no settings you need to do. The Audit Trail is created automatically and cannot be disabled.

To manually send the Audit Trail please refer to Card Interface vendor. Also, to set the address of the centralized log server refer to the Card Interface vendor.

To transmit the Audit Trail the terminal uses the IPOS message called SR_MESSAGE as described in requirement M31054 in document "iPOS_Messages and Commands version 3.2", reference 6. For a detailed

description please refer to reference 8 “Point IPOS - Audit logging” and reference 7 “Terminal Audit Logs File Format “.

Forwarding log to a central log server need to be implemented and provided by the SACI provider.

**Requirement 11: Regularly test security systems and processes**

***a. What the requirement says***

“Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.”, reference 2.

***b. How your Verifone iPOS helps you meet this requirement***

Your Verifone iPOS has mechanisms to ensure that software and parameters can be downloaded from trusted sources only. These mechanisms are based on cryptographic signatures and MAC protection (Message Authentication Code).

***c. What this means to you***

You should test your network connections (including wireless networks) periodically for vulnerabilities, and make use of network vulnerability scans. If you make any significant changes to your network, you should also test for vulnerabilities

## 2.6. Maintain an Information Security Policy

**Requirement 12: Maintain a policy that addresses information security for all personnel**

***a. What the requirement says***

“A strong security policy sets the security tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of Requirement 12, “personnel” refers to full-time and part-time employees, temporary employees, contractors and consultants who are “resident” on the entity’s site or otherwise have access to the cardholder data environment.”, reference 2.

***b. How your Verifone iPOS helps you meet this requirement***

**----**

***c. What this means to you***

----

# 3. How to set up your Verifone iPOS to ensure PCI DSS compliance

## 3.1. Do not retain full magnetic stripe or card validation code

There is no prior software installation on this type of terminal that would be none PCI PA-DSS compliant and therefore there would not be any sensitive historical data inside the terminal. The only upgrade to this software is by physically replacing any prior installation of other types of terminals or new installations.

If it is a replacement of an old unit any old units must be returned to Verifone, since it may contain sensitive historical data.

You must make sure that the software version of the Verifone iPos Payment Core that runs on your Verifone iPOS is listed on the PCI web site "List of Validated Payment Applications" that have been validated in accordance with PCI PA-DSS.

http://www.pcisecuritystandards.org

In order for your organization to comply with PCI DSS requirements it is absolutely necessary to remove historical data stored prior to installing your PCI PA-DSS compliant Verifone iPOS terminal. Therefore you must make sure that historical data (magnetic stripe data, cardholder data and CVV2s) are removed from all storage devices used in your system, ECRs, vending machines, PCs, servers etc. For further details please refer to your vendor.

No specific setup of your Verifone iPOS PCI PA-DSS compliant terminal is required. PAN is stored either truncated or encrypted. Full magnetic stripe data is deleted immediately after authorization and never stored. CVV2 is never used in the terminal since manual entry of PAN is not implemented.

However, if you need to do a voice referral you should never write down or otherwise store PAN, expiration date or CVV2. Collect this type of data only when absolutely necessary.

To comply with the PCI DSS requirements you should never store any sensitive card data such as full track data, CVV2 or PAN, not even for troubleshooting purpose.

## 3.2. Protect stored card holder data

PAN and expiration date are encrypted and stored in a queue in your Verifone iPOS terminal for offline transactions (store and forward). For this encryption a unique key per transaction is used. The queue is stored until the terminal is able to go online or until the queue is emptied by use of a maintenance tool. After the queued transactions are sent to the processor or emptied by the maintenance tool the queue is automatically securely deleted from the Verifone iPOS memory.

To comply with the PCI DSS requirements all cryptographic material must be removed. The removal of this material is handled within the Verifone iPOS and you do not need to take any action.

Verifone iPOS stores encrypted cardholder data in the following files and locations within the terminal:

| **Type of file** | **filename** | **location** |
|---|---|---|
| • Store and Forward queue (S&F) | offline.data | GiD 2 Flash memory |
| • Journal | log.data | GiD 2 Flash memory |

### 3.3. Protect wireless transmissions

If you are using wireless network within your business you must make sure that firewalls are installed that deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the Verifone iPOS environment. Please refer to your firewall manual.

In case you are using a wireless network you must also make sure that:

- Encryption keys were changed from vendor defaults at installation.
- Encryption keys, passwords and SNMP strings are changed anytime someone with knowledge of the those leaves the company or changes position.
- Default SNMP community strings on wireless devices were changed
- Default passwords/passphrases on access points were changed
- Firmware on wireless devices is updated to support strong encryption for authentication and transmission over wireless networks, for example IEEE 802.11i. Please note that the use if WEP as a security control is prohibited.
- Other security related wireless vendor defaults were changed.

### 3.4. Facilitate secure remote software updates

The software of your Verifone iPOS could be updated remotely and automatically. For connection to external networks it is recommended to use firewall protection as per ”2.1 Build and Maintain a Secure Network” in this document. The terminal should not be placed in an Internet accessible network zone (“DMZ”).

Also the security part of the software that resides in the PED (PIN Entry Device) part of the terminal could be updated remotely. The Terminal Management System that is used for distribution of the PED software should be evaluated by a QSA as part of any PCI DSS assessment.

### 3.5. Encrypt sensitive traffic over public networks

Your Verifone iPOS allows transmission over public networks, e.g. public internet. To protect sensitive data your Verifone iPOS uses triple DES encryption with a unique key per transaction. In order to connect your Verifone iPOS to public networks the communication client must use strong cryptography, see reference 9 “NIST SP 800-57 Part 1”.

## 4. Back-out or product de-installation procedures

The software of your Verifone iPOS could be updated remotely either automatically or manually triggered. In the unlikely event that your newly downloaded software fails or malfunctions please contact your TMS operator in order to allow you to download an older version of the software.

# 5. Terminology and abbreviations

| | |
|---|---|
| **Cardholder Data** | PAN, Expiration Date, Cardholder Name (not used by Verifone iPOS) and Service Code. |
| **CVV2** | Card Verification Value, also called CVC2, is a three or four digit value printed on the back of the card but not encoded on the magnetic stripe or the chip. |
| **ECR** | Electronic Cash Register |
| **HTTPS** | Hypertext Transfer Protocol Secure (HTTPS) is a combination of the Hypertext Transfer Protocol with the SSL protocol to provide encrypted communication and secure identification. |
| **Magnetic Stripe Data** | Track data read from the magnetic stripe, magnetic-stripe image on the chip, or elsewhere. |
| **PAN** | Primary Account Number. PAN, also called card number, is part of the magnetic stripe data and is also printed or embossed on the card. PAN can also be stored in the chip of the card. |
| **PCI DSS** | Payment Card Industry Data Security Standard, the subject of this document. Retailers that use applications to store, process or transmit payment card data are subject to the PCI DSS standard. |
| **PCI PA-DSS** | Payment Card Industry Payment Application Data Security Standard is a standard for validation of payment applications that store, process or transmit payment card data. Applications that comply with PA DSS have built in protection of card data and hereby facilitates for retailers to comply with PCI DSS. |
| **PED** | PIN Entry Device. |
| **PIN** | Personal Identification Number. Secret numeric password known only to the user and a system to authenticate the user to the system. |
| **PSP** | Payment Service Provider offers merchants online services for accepting electronic payments. |
| **Sensitive Authentication Data** | Magnetic Stripe Data, CVV2 and PIN. |
| **Service Code** | A three digit code from the magnetic stripe data defining (1) Interchange and technology, (2) Authorization processing and (3) Range of services and PIN requirements. |
| **SNMP** | Simple Network Management Protocol, is a network protocol. It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention. |
| **SSH** | Secure Shell (SSH) is a network protocol that allows data to be exchanged using a secure channel between two networked devices. |
| **SSL** | Secure Sockets Layer is a commonly used method to protect transmission across public networks. SSL includes strong encryption. |
| **TCP** | Transmission Control Protocol is one of the core protocols of the Internet protocol suite. |
| **TMS** | Terminal Management System. |
| **UDP** | User Datagram Protocol is one of the core protocols of the Internet protocol suite. |
| **WEP** | Wired Equivalent Privacy, a wireless network security standard. Sometimes erroneously called "Wireless Encryption Protocol" |
| **WPA** and **WPA2** | Wi-Fi Protected Access, is a certification program created by the Wi-Fi Alliance to indicate compliance with the security protocol created by the Wi-Fi Alliance to secure wireless computer networks. |

# Appendix A Version methodology

## 1. Overview

There are three types of version identifiers related to this project:

- Software package version
- Application package version
- Payment core version

### 1.1. Software package version

The *software package version* identifies a complete set of application files and resource files needed to get a fully operable terminal. At present it consists of the following file types:

- Boot application
- Security application
- Financial application
- GUI server

### 1.2. Application package version

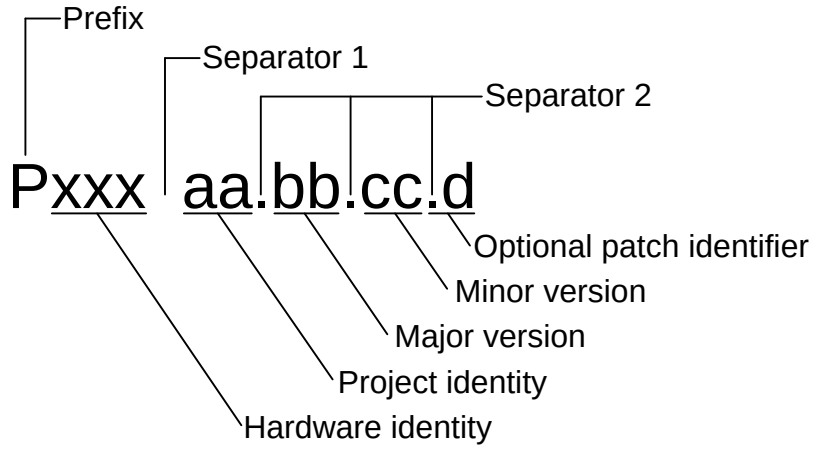
The *application package version* is the version of each individual application.

### 1.3. Payment core version

The *payment core version* is the version of the software modules (inside an application) that have access to clear text card holder data or clear text sensitive authorization data. This is the identifier used for PA-DSS approval.

## 2. Software package

The software package is named according to Point standard naming convention:



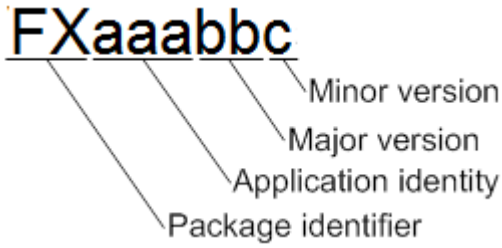

| Field | Format |
|---|---|
| Prefix | One character, always ‘P’ |
| Separator 1 | One character, always space |
| Separator 2 | One character, always . |
| Hardware identity | 3 digit number in range 000 to 999 |
| Project identity | 2 digit number in range 00 to 99 |
| Major version | 2 digit number in range 00 to 99 |
| Minor version | 2 digit number in range 00 to 99 |
| Patch identifier | One character in range ‘a’ to ‘z’ |

Wildcards are not allowed to be used in any field.
The hardware identity for this project is 170 and the project identity are 81-84 and 88–89 for VX820 and project 180 and project identity are 81-84 and 88-89 for VX825.
**Major version** is increased for each new release taken into production or when there are significant changes of the terminal behavior or when the payment core version is changed. Major version is not increased when a patch is taken into production.
**Minor version** is increased for each new release where the major version is unchanged. If major version is changed the minor version will restart at 01.
**Patch identifier** is normally only used during the initial development to prevent us from consuming a lot of versions.

# 3. Application package

An application package name consists of 8 characters according to description below. The name is limited to 8 characters in order to be compatible with the common format for program and parameter download used in Sweden, see ref 2 for details.

## 3.1. Financial application




| Field | Format |
|---|---|
| Package identifier | Two characters, 'FX' are used as identifier for financial application. |
| Application identity | Three numeric characters, see 3.1.1. |
| Major version | Two alphanumeric characters, see 3.1.2 |
| Minor version | One alphanumeric characters, see 3.1.2 |

Wildcards are not allowed to be used in any field.

### 3.1.1. Application identity

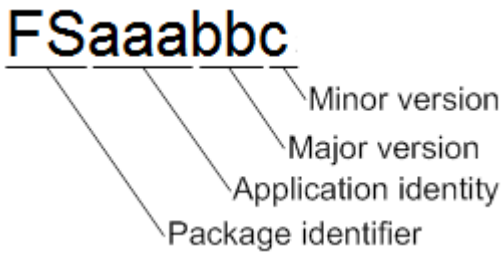
| Application identity | Usage |
|---|---|
| 251 | Sensitive Data Protection Level 1. |
| 252 | Sensitive Data Protection Level 2. |
| 253 | Sensitive Data Protection Level 1, Draft Capture. |
| 254 | Sensitive Data Protection Level 2, Draft Capture. |
| 255 | Wayne Norway |

### 3.1.2. Application version

This field is used differently depending on whether it is a *test-version* or *production-version* of the application. In most cases both application types are identical but a test-version can contain additional functions for debugging purposes.
A *test-version* is identified by a major version starting with an uppercase letter followed by one letter or number. The minor version is always an uppercase letter. The first application created will have version **P0A**.
A *production-version* use 2 digit major version followed by one digit minor version. The first production version created will have version **010**.

**Major version** is increased for each new release taken into production or when there are significant changes of the terminal behavior or when the payment core version is changed. Major version is not increased when a patch is taken into production.
**Minor version** is increased for each new release where the major version is unchanged. If major version is changed the minor version will restart at 01.

## 3.2. Security application




| Field | Format |
|---|---|
| Package identifier | Two characters, 'FS' are used as identifier for security application. |
| Application identity | Three numeric characters, see 3.2.1 |
| Major version | Two numeric characters, see 3.2.2 |
| Minor version | One numeric character, see 3.2.2 |

Wildcards are not allowed to be used in any field.

### 3.2.1. Application identity

| Application identity | Usage |
|---|---|
| 001 | SFEA standard security application. |
| 002 | START standard boot application. |
| 004 | SFEA Norway Esso security application. |
| 005 | SFEA Norway YX security application |

### 3.2.2. Application version

This field is used differently depending on whether it is a *test-version* or *production-version* of the application. In most cases both application types are identical but a test-version can contain additional functions for debugging purposes.
For production version the Minor version is always set to 0 (zero) and the Minor version is only 1-9 for the test versions. If the test versions are more than 9 the Major version is incremented with 1 and the next test version is set to 1.
First test version will have 00 as Major version and 1 as Minor version. The first production version will have 01 as Major version and 0 as Minor version.

## 3.3. Version methodology financial application

Due to the limited characters available the application version methodology might look complicated but it is best illustrated by an example:

1. The application is developed until the first version is ready for test. At that time a *test-version* of the application is created. This application will have version **P1A**.

2. The application does not pass integration test so a new version is developed. For this version the minor version is increased, giving version **P1B**.

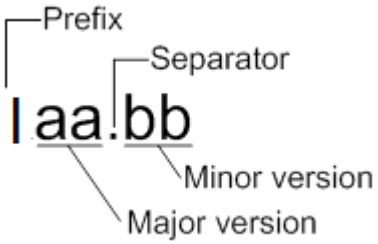
3. The development/test process is repeated (increasing the minor version for each release and optionally increasing the major version if minor version reaches Z) until test version **P1E** is approved to be taken into production. This first production version will have version **010.**

4. Development continues but for the next release of a test-version the major version is increased and the minor version is reset to A (**P2A**).

5. Development/test iteration continues and finally test-version **P2D** is approved to be taken into production as production version **020**.

# 4. Payment core

Payment core use the following naming convention:




| Field | Format |
|---|---|
| Prefix | One character, 'I' |
| Separator | One character, always . |
| Major version | 2 digit number in range 01 to 99 |
| Minor version | 2 digit number in range 00 to 99 |

The version methodology for Payment Core is defined in the following table:

| A change that have: | Version change | Example |
|---|---|---|
| **no impact on functionality of the application or its dependencies** | No version change | I01.01 -> I01.01 |
| **impact on application functionality but no impact on security or PA-DSS requirements** | Minor version increased | I01.01 -> I01.02 |
| **impact to any security functionality or PA-DSS requirement** | Major version increased | I01.01 -> I02.01 |

First version will be **I01.01.**